UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/566,892	02/01/2006	Jonathan G. Foster	GB030128US	9917

24737 7590 06/03/2009
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
VU, PHY ANH TRAN	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
06/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/566,892	**Applicant(s)** FOSTER ET AL.	
	Examiner PHY ANH VU	**Art Unit** 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 5/19/2009.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-15, 19, 20, 22 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-22 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on 01 February 2006 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/19/2009 has been entered.

Response to Arguments

Applicant's arguments filed 04/02/2009 have been considered but are moot in view of the new ground(s) of rejection.

Further, the Examiner respectfully disagrees with Applicant's arguments on page 9 that Wasilewski fails to disclose or suggest the feature of "wherein the terminal determines whether the one or more applications are encrypted." In column 4, lines 46-48, Wasilewski states, "... It is a function of set-top box 113 to determine whether encrypted instances should be decrypted ..." In this passage, Wasilewski discloses the terminal (set-top box) can determine an application should be decrypted. At least for this reason, it must be able to tell that the corresponding application is in encrypted form because only encrypted applications should be decrypted.

Examiner Notes

Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 1 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The limitation of “the terminal determines whether the one or more applications are encrypted," is not described in the original specification at the time of filing, thus constitutes new matter.

Claim Rejections - 35 USC § 103

Claims 1-5, 7-14, 19, 20, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al (US 6,157,719, hereinafter Wasilewski) and further in view of Heredia (US 2003/0217369 A1).

Regarding claim 1, A method of receiving one or more applications at a terminal in a digital broadcasting system, the terminal having access to an interaction channel which can carry signalling to an external party, the method comprising the steps of:

Wasilewski discloses receiving details concerning the one or more applications *(Col 4, lines 41-45, application is received at set top box or Digital Home Communication Terminal (DHCT) (Col 7, lines 35-36)* ,

authorizing the terminal to access the one or more applications by sending an authorization request (*Col 7, lines 2-6, Entitlement Agent (EA) corresponds to authorizing entity,*); (*Col 9, lines 41-53, wherein the encrypted application's info together with authorization info carried by EMM from the DBDS authorized terminal to access the application). When a user wants to view certain program, such as in the case of pay-per-view event, the user orders the event from the entitlement agent (EA), and the EA corresponds by sending an Entitlement Management Messages (EMM) that contains the necessary authorization information to the user. In doing so, this corresponds to sending the request to the authorizing entity to be authorized (Col 30, lines 41-65)* over the interaction channel to an authorizing entity (*i.e: Col 4, lines 42-44; Col 7, lines 30-33. The communication between the user and the EA is over a channel which corresponds to the interaction channel)*

receiving a key over the interaction channel in response to being authorized (*Col 9, lines 41-55, wherein after the terminal has been authenticated, the key appends to the ECM from the service origination which has been sent through the transmission medium to the terminal is received and used to decrypt the content*) ;

receiving the one or more applications (*i.e: Col 4, lines 41-49; wherein application is received at the terminal)*; and

decrypting the one or more applications using the received key (*Col 4, lines 46-62; Col 9, lines 48-55, control word received is used as key to decrypt the encrypted application*).

wherein the terminal determines whether the one or more applications are encrypted (*i.e: Col 4, lines 46-48*); and

a separate file for each encrypted application or a single file for all encrypted applications (*i.e: Col 4, lines 30-35, 41-45, wherein the details include encrypted program information, and information needed to decrypt the encrypted program.*)

Waskilewski does not disclose the details stored in an Application Information Table (AIT);

However, **Heredia discloses** the details stored in an Application Information Table (AIT) (*i.e: [0075]-[0077]*)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Heredia into the method of Wasilewski to provide a flexible way of creating, transmitting and using the application information (Heredia, abstract).

Regarding claim 2, Wasilewski also discloses the step of receiving the details concerning the one or more applications (*Col 4, lines 30-35, 41-45; wherein the details include encrypted program information, and information needed to decrypt the encrypted program)* comprises receiving a launcher application (*Col 5, lines 1-6; corresponds to EMM,*) which is arranged to authorize the terminal (*Col 4, lines 64-67; Col 5, lines 1-6; Col 6, lines 32-33, 39-42, 56-60; wherein EMM contains information to authorize the terminal*).

Regarding claim 3, Wasilewski also discloses the method according to claim 1 wherein the step of receiving the details concerning the one or more applications (*Col 4, lines 30-35,41-45; wherein the details include encrypted program information, and information needed to decrypt the encrypted program)* comprises receiving a launcher application (*corresponds to EMM, Col 5, lines 1-6*) which is arranged to decrypt each encrypted application (Col 6, lines 32-33, 39-42, 56-64; *Col 9, lines 41-55, wherein, after the terminal has been authenticated by EMM, the authenticated information in*

EMM is used in combination with the key carried by ECM to decrypt the encrypted application)

Regarding claim 4, Wasilewski also discloses the method according to claim 2 wherein the launcher application (*corresponds to the EMM, Col 5, lines 1-6*) is received via a different delivery channel to each encrypted application (*Col 5, lines 6-9; Col 10, lines 62-64*).

Regarding claim 5, Wasilewski also discloses the method according to claim 1 wherein the step of decrypting each encrypted application is performed by an application loader (*Col 9, lines 40-55; wherein when the key is used to decrypt the encrypted content to produce original content, it is also loading the application*).

Regarding claim 7, Wasilewski also discloses the method according to claim 1 wherein the received details include one or more of: an encryption method used to encrypt the application; cost of the application; payment details (*Col 16, lines 11-14; Col 30, lines 58-65; Col 31, lines 27-29; Col 32, lines 63-67, Col 33, lines 1-8; wherein the purchase information which includes the cost of the application is provided to the user*).

Regarding claim 8, Wasilewski also discloses the method according to claim 1 further comprising the step of collecting payment details from a user of the terminal (*Col 32, lines 63-67; Col 33, lines 1-9; wherein the details include checking the cost of the application to make sure it doesn't exceed the user's limit, then the cost is added to the user's current credit balance*).

Regarding claim 9, Wasilewski also discloses the method according to claim 1 further comprising the step of collecting payment from a user of the terminal (*Col 33, lines, 7-9; wherein the cost is added to the user's current credit balance*).

Regarding claim 10, Wasilewski also discloses the method according to claim 1 wherein the terminal has a public/private key pair and the step of contacting an external party comprises sending the public key to the external party (Col 11, lines 57-60; *Col 5, lines 27-34, wherein, an entity provides its public key to any other entity that wants to communicate with it*).

Regarding claim 11, Wasilewski also discloses the method according to claim 10 further comprising receiving a decryption key from the external party which has been encrypted using the public key (Col 5, lines 27-34; Col 6, lines 32-33, 40-42, 60-62; *Col 9, lines 40-55; wherein the decryption key is received at the terminal from ECM, which corresponds to external party, that has been encrypted using the terminal's public key).*

Regarding claim 12, Wasilewski also discloses the method according to claim 10 wherein the public/private key pair uniquely identifies the terminal (Col 11, lines 57-60; *Col 8, lines 39-43, 51-54, wherein private key have to correspond to public key of the terminal in order to decrypt the encrypted information*).

Regarding claim 13, Wasilewski also discloses the method according to claim 10 wherein the public key is signed by a manufacturer of the terminal (*Col 11, lines 58-60; wherein keys are installed in the terminal at the time it was manufactured*).

Regarding claim 14, Wasilewski discloses the method according to claim 1 wherein the digital broadcasting system does not use a conditional access (CA) system (*i.e*: *Col. 30, lines 41-67; Col 31, lines 1-10, wherein broadcast events, impulse pay-per-view, and pay-per-view events are available to customers who don't have to subscribe to a monthly basis, but rather, on a per event basis, which corresponds to the broadcasting system that does not use conditional access (CA) as claimed here*).

Regarding claim 19, Wasilewski also discloses a method of transmitting one or more applications to a terminal (*Col 4, lines 41-49; Col 9, lines 25-26; wherein encrypted program is sent to set top box*) in a digital broadcasting system (*Fig. 6, illustrates the Digital Broadband Delivery System*), the terminal having access to an interaction channel which can carry signalling to an external party (*Col 4, lines 42-44; Col 7, lines 30-33, transmission medium, such as wire, coaxial cable, or fiber optic cable is used to carry messages from Digital Broadband Delivery System (Col 14, lines 34-35, corresponds to external party) to the set top box*), the method comprising the steps of:

transmitting details about the one or more applications (Col 9, lines 25-40; *Col 4, lines 27-35, 41-42; wherein the details include encrypted program information, and information needed to decrypt the encrypted program*), including a launcher application (*corresponds to EMM, Col 5, lines 1-6*) which is arranged to authorize the terminal to access the one or more applications by sending an authorization request over the interaction channel to an authorizing entity (*Col 4, lines 64-67; Col 5, lines 1-6; Col 6,* *lines 32-33, 39-42, 56-60; Col 9, lines 41-53; wherein the encrypted application's info together with authorization info carried by EMM from the DBDS authorized terminal to access the application. When a user wants to view certain program, such as in the case of pay-per-view event, the user orders the event from the entitlement agent (EA), and the EA corresponds by sending an EMM that contains the necessary authentication information to the user. In doing so, this corresponds to the user sending a request to the authorizing entity to be authorized (Col 30, lines 41-65). The communication between the user and the EA is over a channel (corresponds to the interaction channel, Col 4, lines 43-44; Col 7, lines 30-31)*;

receive a key over the interaction channel in response to being authorized (Col 6, lines 32-33, 40-42, 60-62; *Col 9, lines 40-55; wherein EMM contains information to authorize the terminal*);

decrypt the one or more applications using the key (Col 5, lines 27-34; Col 6, lines 32-33, 40-42, 60-62; *Col 9, lines 40-55; wherein, after the terminal has been authenticated by EMM, the authenticated information in EMM is used in combination with the key carried by ECM to decrypt the application*); and,

transmitting the one or more applications (Col 9, lines 25-40; *Col 4, lines 27-35, 41-42, wherein application is sent to set top box*).

wherein the terminal determines whether the one or more applications are encrypted (*i.e: Col 4, lines 46-48*); and contains a separate file for each encrypted application or a single file for all encrypted applications (*i.e: Col 4, lines 30-35, 41-45, wherein the details include encrypted program information, and information needed to decrypt the encrypted program.*)

Waskilewski does not disclose the details stored in an Application Information Table (AIT);

However, **Heredia discloses** the details stored in an Application Information Table (AIT) (*i.e: [0075]-[0077]*)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Heredia into the method of Wasilewski to provide a flexible way of creating, transmitting and using the application information (*Heredia, abstract*).

Regarding claim 20, Wasilewski discloses a machine-readable medium storing a set of programmable instructions configured for execution by at least one processor for providing for one or more applications for transmission to a terminal in a digital broadcasting system, the method comprising the steps of:

providing the terminal with access to an interaction channel which can carry signalling to an external party (*Col 4, lines 42-44; Col 7, lines 30-33, transmission medium, such as wire, coaxial cable, or fiber optic cable*), the one or more applications comprising a launcher application (*corresponds to EMM, Col 5, lines 1-6*) comprising code (*Col 18, lines 2-6, wherein EMM contains a message authentication code*) which, when executed by a processor in the terminal, causes the processor to perform the steps of:

transmitting details about the one or more applications (Col 9, lines 25-40; *Col 4, lines 27-35, 41-42, wherein application is sent to set top box*)

authorizing the terminal to access the one or more applications by sending an authorization request over the interaction channel to an authorizing entity (*Col 4, lines 64-67; Col 5, lines 1-6; Col 6, lines 32-33, 39-42, 56-60; Col 9, lines 41-53; wherein the encrypted application's info together with authorization info carried by EMM from the DBDS authorized terminal to access the application). When a user wants to view certain program, such as in the case of pay-per-view event, the user orders the event from the entitlement agent (EA), and the EA corresponds by sending an EMM that contains the necessary authentication information to the user. In doing so, this corresponds to the user sending the request to the authorizing entity to be authorized (Col 30, lines 41-65). The communication between the user and the EA is over a channel (corresponds to the interaction channel, Col 4, lines 43-44; Col 7, lines 30-31),* and to receive a key over the interaction channel in response to being authorized (Col 5, lines 27-34; Col 6, lines 32-33, 40-42, 60-62; *Col 9, lines 40-55; wherein EMM contains information to authorize the terminal)* ; and, decrypting the one or more applications using the received key (Col 6, lines 32-33, 39-42, 56-64; *Col 9, lines 41-55, wherein, after the terminal has been authenticated by EMM, the authenticated information in EMM is used in combination with the key carried by ECM to decrypt the encrypted application*).

wherein the terminal determines whether the one or more applications are encrypted (*i.e: Col 4, lines 46-48*); and

contains a separate file for each encrypted application or a single file for all encrypted applications (*i.e: Col 4, lines 30-35, 41-45, wherein the details include encrypted program information, and information needed to decrypt the encrypted program.*)

Waskilewski does not disclose the details stored in an Application Information Table (AIT);

However, **Heredia discloses** the details stored in an Application Information Table (AIT) (*i.e: [0075]-[0077]*)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Heredia into the method of Wasilewski to provide a flexible way of creating, transmitting and using the application information (*Heredia, abstract*).

Regarding claim 22, Wasilewski discloses a method of transmitting one or more applications to a terminal (*Col 4, lines 41-49; Col 9, lines 25-26; wherein encrypted* *program is sent to set top box*) in a digital broadcasting system (Fig. 6) in which a conditional access (CA) system is not in use (*i.e: Col. 30, lines 41-67; Col 31, lines 1-10, wherein broadcast events, impulse pay-per-view, and pay-per-view events are available to customers who don't have to subscribe to a monthly basis, but rather, on a per event basis, which corresponds to the broadcasting system that does not use conditional access (CA) as claimed here*) *"users can simply pay for whatever application they desire without an ongoing subscription commitment" which examiner interpret this as corresponding to pay-per-view, or Impulse pay-per-view.* , the method comprising:

transmitting unencrypted details about the one or more applications (Col 42, lines 11-19);

wherein the terminal determines whether the one or more applications are encrypted (*i.e: Col 4, lines 46-48*); and

contains a separate file for each encrypted application or a single file for all encrypted applications (*i.e: Col 4, lines 30-35, 41-45, wherein the details include encrypted program information, and information needed to decrypt the encrypted program.*)

Waskilewski does not disclose the details stored in an Application Information Table (AIT);

However, **Heredia discloses** the details stored in an Application Information Table (AIT) (*i.e: [0075]-[0077]*)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Heredia into the method of Wasilewski to provide a flexible way of creating, transmitting and using the application information (*Heredia, abstract*).

Claim 6, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al (US 6,157-719, hereinafter Wasilewski) in view of Heredia (US 2003/0217369) and further in view of Peng et al., "Digital Television Application Manager" 2001 IEEE International Conference on Multimedia and Expo (Hereinafter, Peng).

Regarding claim 6, Wasilewski discloses all the limitations of claim 6, except wherein the application loader is a Java ClassLoader.

However, **Peng discloses** Java ClassLoader (*Page 687*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the feature of Java ClassLoader as discussed in Peng into the method of Wasilewski and Heredia, because it would provide for the purpose of loading application classes from different sources and solve name collisions (*Page 688, 4th paragraph*)

Regarding claim 15, Wasilewski discloses all the limitations of claim 15, except the digital broadcasting system is the Multimedia Home Platform (MHP).

However, **Peng discloses** the digital broadcasting system is a Multimedia Home Platform (MHP) (*Page 685*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the feature of MHP as discussed in Peng into the system of Wasilewski, because MHP is being used as a common platform for user to transparently access a range of multimedia services (Page 685, 2nd paragraph).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHY ANH VU whose telephone number is (571)270-7317. The examiner can normally be reached on Mon-Thr 7:30-5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/PHY ANH VU/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437